Codify
BY AAPC

Health Information Compliance Alert

Know What Happens During a Forensic Investigation

Tip: Don't destroy evidence.

Whether you decide - or the feds require you - to hire forensic investigators to evaluate a breach, there are certain things you can do to prepare ahead of time.

For example, experts warn organizations to stop the incident, but keep the proof intact.

"First, contain the breach," says **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. "Don't wipe affected systems because you might destroy evidence needed by the forensic team to determine what [electronic protected health information] ePHI was compromised and how to prevent it from happening again."

Adam Kehler, CISSP, principal consultant and healthcare practice lead with **Online Business Systems** agrees. "When an organization finds out they have an incident such as ransomware, the temptation is to immediately power down the systems and wipe drives. In doing so, they may actually be destroying evidence that could be useful in investigating the incident," he adds.

Evaluate the Breach Level

Depending on the severity of the data security incident, the parties involved, and the information usurped, you may need to get the authorities involved. More significant and nefarious breaches may warrant a call to your local law enforcement agency or the **Federal Bureau of Investigation** (FBI), counsels Kehler.

It's a good idea to get in touch with your IT vendors and cyber insurers, too. And if the breach is major, a lawyer might be next in line of those to contact.

"These resources can help determine the most appropriate steps to take to ensure that they are able to limit the impact and quickly recover while maintaining evidence and meeting their compliance requirements," Kehler says.

Take a Look at the Timeline

If cybersecurity experts, law enforcement, or the **HHS Office for Civil Rights** (OCR) think that a forensic investigation may help, several things will follow.

Consider this expert advice on what to expect:

Prepare for an in-person audit: "A forensic team will typically come onsite to your practice and carefully evaluate the state of your systems," says Stone. They'll do this "so you know exactly what happened and how the breach occurred," she explains.

Get ready for an in-depth review: The investigation will look closely at your IT products, machines, and protocols. This analysis will help the team determine the nitty gritty of the breach.

Understand these investigation logistics: "This evaluation is typically performed by taking an image and memory dump of affected systems," maintains Kehler. "The investigation is performed on these images and dumps in order to avoid tampering with the evidence and maintaining chain of custody."

Keep systems up and running: Your first inclination may be to shut everything down, but that's not a good idea. When you power off, the memory will be lost - and that could have catastrophic repercussions. "Many malware systems

these days never write to disk; they are located in memory only," Kehler says.

Take the forensic team's advice seriously: This kind of investigation is usually required after a costly, complicated cyber attack, so it is critical to work with the forensic team and listen to their instructions to eradicate problems. "They will tell you what you need to know to remediate the issue and offer recommendations for implementing security controls that will prevent future breaches," instructs Stone.